How will the coronavirus contact-tracing apps work?

PC Probe

How will the coronavirus contact-tracing apps work?

Apps to combat Covid-19 are riddled with practical pitfalls and privacy problems, Stewart Mitchell finds

Governments globally are turning to technology to fight Covid-19, but experts fear the apps designed to counter the virus could bring serious problems of their own.

The UK, like many other countries, has set up a taskforce to build a contact-tracing app that identifies when a known Covid-19 carrier comes into contact with someone else. The app flags contact points and allows potentially newly infected patients to seek medical advice or to self-isolate.

Singapore, for example, released its app in March and European countries are working on their own systems, due for release in the coming weeks, but all will face the same problems of balancing efficacy against the constraints of technology and privacy.

According to Claudia Pagliari, director of global eHealth at the University of Edinburgh, the ethical dilemmas such apps bring are far from new, but she fears such concerns will be sidelined in the rush to release the contact tracers.

"For notifiable diseases that present a threat to others, consent and confidentiality can take second place to public health, and the privacy rights of individuals can take second place to the rights of those they may have infected," she said.

She warns: "The increasing role of technology companies in the era of Covid-19, along with branches of government outside healthcare, is shaping these trade-offs in new ways, as we begin to lose sight of who is controlling our information and choices."

Although there is public support, in principle, for a UK contact-tracing app (65% approval, according to Ipsos Mori), the government is having to finely balance its desire for more data about our symptoms, contacts and location, against the risk of public anxiety over state surveillance.

Against this backdrop, the unlikely couple of Apple and Google have teamed up to present a solution based on Bluetooth beacons embedded in mobile phones. Although it's similar to other Contact Tracing Frameworks (CTFs) proposed by academic and industry consortia, the Apple/Google approach is emerging as the frontrunner.

The system enables cryptic anonymised codes to be exchanged between phones in close proximity, to create a record of contacts without the need for centralised tracking. "Their tech includes no location data, keeps

Who gets to see the app data?

If trackers and apps are optional, as currently legislated in the UK, how many people download them remains to be seen. Much will depend on the level of trust officials can build in the service.

On top of the Apple/Google project, the government is exploring how to link these tools to sources of identifiable data, such as electronic medical records, to allow researchers to study the effects of factors such as geography, existing health conditions or ethnicity on outcomes. However, this risks breaching the public trust that's critical to such a scheme's success.

"These secondary uses may have value, but it's incumbent upon the government to be honest with the public about the aims of all this data gathering, and who else stands to benefit, such as companies or researchers with a stake in the systems or analytics," said Claudia Pagliari.

While the NHS is a trusted body, concerns have been raised about some of the companies the UK government has chosen to partner with during the crisis, in particular Palantir.

In the announcement about the taskforce, health officials explained that Palantir Technologies UK was providing software that "enables disparate data to be integrated, cleaned, and harmonised in order to develop the single source of truth that will support decision-making".

Assurances have been given that Palantir is "not a data controller, and cannot pass on or use the data for any wider purpose without the permission of NHS England".

But people who have followed Palantir's work for the US's immigration enforcement agency may be more cautious. "When Palantir's involvement was announced, it was framed like a benign data plumber to help with the coronavirus effort," said Pagliari. "But they are actually data miners, and their main business lies in the crime/security/forensics sector, with many government contracts for policing and anti-terrorism activities."

According to Pagliari, the firm's involvement implies the possibility of stricter electronic measures being imposed if the crisis deepens. "The appearance of Palantir and similar firms in the coronavirus effort hints at preparations for more extreme forms of surveillance and control, should the public rebel against social distancing or if mass infection breaks out," she said. "Hopefully, with the flattening of the curve, any such ambitions will be shelved."

everything on your phone unless you're a part of a reported infection, [and] protects personal anonymity via a random ID issued to you every day," said Craig Danuloff, CEO of privacy software firm The Privacy Company in a blog post.

"What they're proposing is less privacy-invasive than using maps. It's less privacy-invasive than having a Facebook account. It's purpose-driven, narrowly focused, privacy-centric, and will exist only while we need it."

Even long-standing privacy advocates argue that compromises have to be made when dealing with situations such as Covid-19. "The expectation of privacy around tracing contacts of someone who's got a notifiable disease is very much less [than normal]," Ross Anderson, professor of security engineering at the Department of Computer Science and Technology, University of Cambridge, told *PC Pro*. "It's a mistake to conflate this with online anonymity.

"A doctor who diagnoses you must inform the public health authorities, and if they have the bandwidth, they call you and ask who you've been in contact with. They then call your contacts in turn," he said.

Is Bluetooth up to the job?

While Bluetooth solutions might please privacy watchdogs, experts have pointed to limitations in the underpinning technology, which was initially developed for the advertising industry.

For a start, researchers believe as many as two billion handsets globally can't use the low-power Bluetooth beacons that drive the Apple/Google project because older handsets don't support the technology, immediately hampering a system that needs to reach a critical mass of users to be effective.

There are further concerns about accuracy. "When Bluetooth low-energy beacons were designed, it was binary: 'Can you see the device or not?'" said Phil Booth, coordinator of health rights group medConfidential. "They're now trying to go to a completely different level of sophistication to determine what distance you are from the beacon.

"The basic concept of what they are trying to do is infer a distance and measure a time and combine those two data points as a proxy for infection, but doing so uses huge assumptions, so there could be huge amounts of dirty or plain false information."

Even if apps can be coded to work around this issue, the vast array of hardware could also impact the quality of results. In the same way that mobile phone models display different signal strengths in the same location, Bluetooth reception also varies.

ABOVE Without widespread testing, many carriers will be left untraced

"It's one thing to say 'beacons allow you to infer a range down to 2m', it's completely another thing when you run that protocol across different hardware platforms," said Booth. "How do you know the algorithm you're running when broadcast to an iPhone 6 is going to deliver exactly the same range proximity measurement as when it's broadcast into a Samsung?

"It's not a simple case of code, this is about chipsets and performance of hundreds of different devices and versions of devices and chipsets."

Mixed measurements are further complicated by environmental factors. For example, a Bluetooth beacon won't distinguish whether someone is wearing a mask, or is even in the same room as the carrier, because the radio waves pass through walls. Anderson suggests that a way to improve the quality of the data would be to use an app to "involve each user, presenting them with a list of possible significant contacts (whatever the criterion for that is, say, within 2m for five minutes) and let them delete those that are not relevant, perhaps for people in other rooms."

> "This is about chipsets and performance of hundreds of different devices and versions of devices and chipsets"

However, a system that relies on users to confirm contact with infected patients also runs the risk of people falsely reporting so that they can continue working or avoid self-isolation.

A more fundamental problem for the feasibility of contact-tracing technology is the absence of reliable data on who is carrying the disease. "Consider how few people are actually being tested, compared with the many thousands likely to be affected," said Pagliari. "Given the scarcity of lab tests up until now, most of those confirmed positive for Covid-19 are serious cases admitted to hospital, which begs the question: who's contacts are you going to trace?" she added. "Without knowing who's infected in the first place, expecting everybody to install these trackers on their phones makes little sense unless you have other uses in mind." ●